Notice of Allowability	Application No.	Applicant(s)	
	10/588,188	KEENI, GLENN MANSFIELD	
	Examiner	Art Unit	
	NARCISO VICTORIA	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *3/21/2011*.

2. ☒ The allowed claim(s) is/are *10-15,20-22,24 and 25*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 4/01/2011
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/N. V./ Examiner, Art Unit 2438	

DETAILED ACTION

The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior Office actions.

The prior Office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

Claims 10-15 and 20 have been amended; claims 16-19 have been cancelled; claims 1-9, 23 and 26 have been previously cancelled.

Claims 1-25 are now re-numbered as claims 1-11.

Information Disclosure Statement

The Information Disclosure Statement (IDS) submitted on April 1, 2011 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the IDS statement has been considered by the Examiner.

EXAMINER'S AMENDMENT

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with JEREMY MERENESS, Registration # 63,422, on June 1, 2011.

The Application has been amended as follows:

Abstract

~~There is provided~~ A system for detecting and tracing a (D)DoS attack and identifying the attack source, which system simplifies the judgment reference to determine whether a (D)DoS attack is present. The number of source addresses of the ~~packets~~ packets transmitted via the [[.]] Internet line is monitored. When the number of the source addresses has reached a predetermined number or a predetermined ratio within a predetermined time, it is judged that an unauthorized attack is present. Moreover, where the hop number of the packet ~~of the HOP number~~ is different from ~~the~~ a hop number corresponding to the transmission source information, the packet is judged to be ~~unauthorized information~~ malicious.

The Claims

10. (Currently Amended) A network attack detection system, comprising ~~processors~~ a hardware communications monitor programmed to perform the steps of:

examining a header of a packet in transmission;

observing values of one or more pre-specified fields in the packet header; and

in a case where a number of distinct values observed in the pre-specified fields reaches a pre-specified threshold suggesting a pre-specified ratio within a pre-specified time interval, judging that an unauthorized attack is in progress;

wherein the judging is carried out based on one of the following conditions where N(t) is the number of distinct values of the field observed within a pre-specified time

interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1, P(t) is a number of packets in transmission within the pre-specified time interval from time t, $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time ~~t, then start listing the alternative conditions~~:

(a) if the ratio of N(t) to $N(t_1)$ is greater than or equal to a first pre-specified threshold k_1, that is, if $N(t) / N(t_1) \geq k_1$, the system will judge that an attack is in progress;

(b) if the ratio of N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t) / P(t) \geq k_2$, the system will judge that an attack is in progress;

(c) if the ratio of $\{N(t) / P(t)\}$ to $\{N(t_1) / P(t_1)\}$, is greater than or equal to a third pre-specified threshold k3, that is, $\{N(t) / P(t)\} / \{N(t_1) / P(t_1)\} \geq k3$, the system will judge that an attack is under progress; or

(d) if the ratio N(t) to T(t) is greater than or equal to a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, the system will judge that an attack is in progress.

11. (Currently Amended) The network attack detection system according to claim 10, wherein the ~~processors are~~ hardware communications monitor is further programmed to perform the further step of:

in a case where numbers of distinct values observed in the pre-specified fields, comprising arbitrary combinations of two or more header fields, reach a pre-specified

threshold within a pre-specified time interval, judging that an unauthorized attack is in progress,

wherein the judging is carried out based on one of the above conditions (a)-(d).

12. (Currently Amended) The network attack detection system according to claim 10, wherein the ~~processors are~~ hardware communications monitor is further programmed to perform the further step of:

in a case where the Time To Live (TTL) value in the header field of the packet does not lie in the range of the values seen beforehand for the source address in the header field of the packet, judging that an unauthorized attack is in progress.

13. (Currently Amended) The network attack detection system according to claim 10, wherein the ~~processors are~~ hardware communications monitor is further programmed to perform the step of:

in a case where numbers of distinct values observed in the pre- specified fields comprising of arbitrary combinations of two or more header fields are greater than, or equal to, one's pre- specified threshold value within a pre-specified time interval, judging that an unauthorized attack is in progress.

14. (Currently Amended) The network attack detection system according to claim 13, wherein the ~~processors are~~ hardware communications monitor is further programmed to perform the step of:

in a case where the Time to Live (TTL) value in the header field of the packet does not lie in the range of the values seen beforehand for the source address in the header field of the packet, judging that an unauthorized attack is in progress.

15. (Currently Amended) A network attack tracking system, comprising:

two or more ~~of the~~ network attack detection systems ~~as claimed as claim 10~~,

wherein a source of the unauthorized attack is searched by deploying said two or more network attack detection systems at various places on the Internet, and

wherein each network attack detection system comprises a hardware communications monitor programmed to perform the steps of:

examining a header of a packet in transmission;

observing values of one or more pre-specified fields in the packet header; and

in a case where a number of distinct values observed in the pre-specified fields reaches a pre-specified threshold suggesting a pre-specified ratio within a pre-specified time interval, judging that an unauthorized attack is in progress;

wherein the judging is carried out based on one of the following conditions where N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1, P(t) is a number of packets in transmission within the pre-specified time interval from time t, $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and T(t) is the

number of octets or bits in the packets in transmission within the pre-specified time interval from some time t:

(a) if the ratio of N(t) to $N(t_1)$ is greater than or equal to a first pre-specified threshold k_1, that is, if $N(t) / N(t_1) \geq k_1$, the system will judge that an attack is in progress;

(b) if the ratio of N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t) / P(t) \geq k_2$, the system will judge that an attack is in progress;

(c) if the ratio of $\{N(t) / P(t)\}$ to $\{N(t_1) / P(t_1)\}$, is greater than or equal to a third pre-specified threshold k3, that is, $\{N(t) / P(t)\} / \{N(t_1) / P(t_1)\} \geq k3$, the system will judge that an attack is under progress; or

(d) if the ratio N(t) to T(t) is greater than or equal to a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, the system will judge that an attack is in progress.

16-19 (Cancelled)

20. (Currently Amended) A method for detecting a network attack, comprising the steps of:

examining a header of a packet in transmission;

observing values of one or more pre-specified fields in the packet header; and

in a case where a number of distinct values observed in the pre-specified field reaches a pre-specified threshold suggesting a pre-specified ratio within a pre-specified time interval, judging that an unauthorized attack is in progress;

wherein the judging is carried out based on one of the following conditions where N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1, P(t) is ~~the~~ a number of packets in transmission within the pre-specified time interval from time t, $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time ~~t_1, then start listing the alternative conditions~~:

(a) if the ratio of N(t) to $N(t_1)$ is greater than or equal to a first pre-specified threshold k_1, that is, if $N(t) / N(t_1) \geq k_1$, the system will judge that an attack is in progress;

(b) if the ratio of N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t) / P(t) \geq k_2$, the system will judge that an attack is in progress;

(c) if the ratio of $\{N(t) / P(t)\}$ to $\{N(t_1) / P(t_1)\}$, is greater than or equal to a third pre-specified threshold k3, that is, $\{N(t) / P(t)\} / \{N(t_1) / P(t_1)\} \geq k3$, the system will judge that an attack is under progress; or

(d) if the ratio N(t) to T(t) is greater than or equal to a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, the system will judge that an attack is in progress.

Response to Arguments

Applicant's arguments filed March 21, 2011 have been fully considered and are persuasive.

Allowable Subject Matter

Claims 10-15, 20-22 and 24-25 are allowed over prior art of record.

Examiner's Statement of Reasons for Allowance

The following is an Examiner's statement of reason(s) for allowance:

Amended independent claims 10, 15 and 20 are allowed in view of the Examiner's Amendment, specification and for reasons argued by the Applicant on pages 17-25 of the "Remarks", filed March 21, 2011, and dependent claims 11-14, 21-22 and 24-25 depend upon one of the above-mentioned allowed claims and are therefore allowed by virtue of their dependency.

Chesla et al. (prior art on the record) discloses a method involving measuring a time related property of a traffic entering a computer network, the traffic being filtered by blocking the traffic characterized by a determined parameter, analyzing the traffic using fuzzy logic algorithm to detect an attack, determining another parameter in response to the analysis, and filtering the traffic by blocking the traffic characterized by both parameters.

Apap et al. (prior art on the record) discloses computer system operation's intrusion detecting method involving analyzing features from record of process that accesses operating system registry to detect deviation from normal computer usage.

Chao et al. (prior art on the record) discloses a method involving confirming a distributed denial of service (DDoS) attack at a network location using a set of packet attribute values, computing an aggregate conditional probability measure for each packet based on selected attributes, computing an aggregate cumulative distribution

function (CDF) of scores based on the measure, and finding a discarding threshold using the function, the discarding threshold being sent to routers.

Applicant's arguments, see "Remarks" pages 17-25, are persuasive as the combination of prior art references fails to teach the claimed invention because of the non-obvious claimed limitations (common to all independent claims) "in a case where a number of distinct values observed in the pre-specified field reaches a pre-specified threshold suggesting a pre-specified ratio within a pre-specified time interval, judging that an unauthorized attack is in progress." None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present Application at or before the time it was filed.

Any comments considered necessary by Applicant(s) must be submitted no later than payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reason(s) for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to NARCISO VICTORIA whose telephone number is (571)270-7904. The Examiner can normally be reached on Monday to Friday 10:00am - 6:00pm EST.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Taghi Arani can be reached at (571)272-3787. The fax phone number for the organization where this Application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/NV/

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438